

PATENT ABSTRACTS OF JAPAN

W1508

(11)Publication number : 09-212565

(43)Date of publication of application : 15.08.1997

(51)Int.Cl.

G06F 19/00

G06K 17/00

G07D 9/00

G07D 9/00

G07D 9/00

G07D 9/00

(21)Application number : 08-020337

(71)Applicant : NEC CORP

(22)Date of filing : 07.02.1996

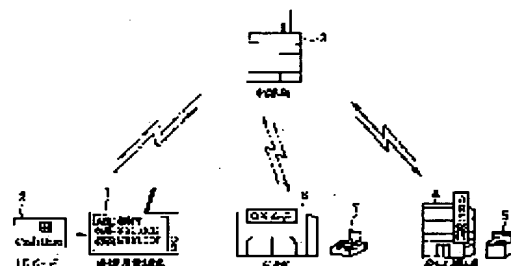
(72)Inventor : WATANABE MITSUHIRO

(54) RADIO PORTABLE TERMINAL SYSTEM

(57)Abstract:

PROBLEM TO BE SOLVED: To make a place where a user is charged unlimited and minimize the possibility that information is stolen by making a radio connection with the center terminal of a financial institution, and exchanging money information and confirming a password code.

SOLUTION: A customer inserts an IC card 2 into the radio portable terminal 1 first and inputs necessary money with input keys on the radio portable terminal 1. Then this information is inputted to the financial institution 4 through a repeater station 3 and the center terminal 5. Then necessary money is withdrawn from the account of the customer of the financial institution 4 and then the IC card 2 of the customer is charged with the money. When the customer makes a purchase at a store 6, the customer carries the IC card 2 to the store 6 and inserts it into a register terminal at the store 6, and then the money of the purchase is withdrawn from the amount of the IC card 2. The store 6 demands the financial institution 4 to pay the money through the register terminal 7, repeater station 3, and center terminal 5 according to the customer information read out of the IC card 2.



LEGAL STATUS

[Date of request for examination]

07.02.1996

[Date of sending the examiner's decision of rejection]

21.09.1999

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's
decision of rejection]

[Date of extinction of right]

Copyright (C); 1998,2003 Japan Patent Office

W1505

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平9-212565

(43) 公開日 平成9年(1997)8月15日

(51) Int.Cl. ⁸	識別記号	庁内整理番号	F I	技術表示箇所
G 0 6 F 19/00			G 0 6 F 15/30	C
G 0 6 K 17/00			G 0 6 K 17/00	L
G 0 7 D 9/00	4 3 6		G 0 7 D 9/00	4 3 6 Z
	4 5 1			4 5 1 B
	4 5 6			4 5 6 A
審査請求 有 請求項の数 9 O L (全 15 頁) 最終頁に続く				

(21) 出願番号 特願平8-20337

(22) 出願日 平成8年(1996)2月7日

(71) 出願人 000004237

日本電気株式会社

東京都港区芝五丁目7番1号

(72) 発明者 渡辺 光洋

東京都港区芝五丁目7番1号 日本電気株式会社内

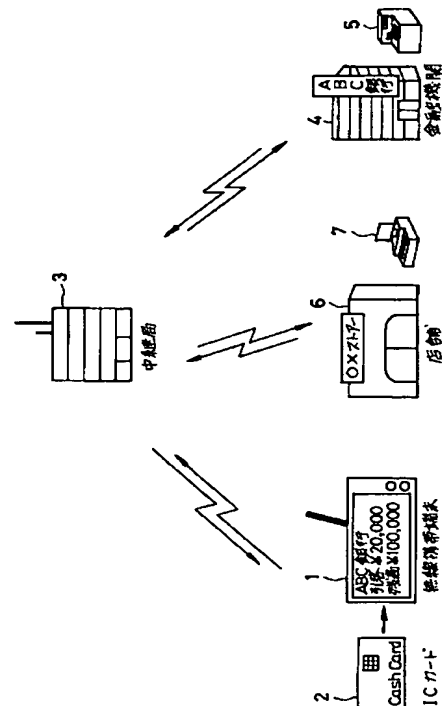
(74) 代理人 弁理士 ▲柳▼川 信

(54) 【発明の名称】 無線携帯端末システム

(57) 【要約】

【課題】 ICカードに金銭をチャージする場所がATMのある場所に限定されること。

【解決手段】 中継局3を介して金融機関4の端末5と無線で接続される無線携帯端末1と、この無線携帯端末1に挿入されるICカード2とで構成され、無線携帯端末1よりICカード2に直接金銭情報を書き換える。また、ICカード2内にチャージされる金銭残高は無線携帯端末1を介して電波により金融機関4の端末5に送信され、金融機関4はこの金銭残高を顧客の口座の残高と照合する。



【特許請求の範囲】

【請求項 1】 金融機関のセンター端末と無線で接続され、金銭情報のやりとりと暗証番号の確認を行うことで金銭情報の引き落としおよび預け入れを行う無線通信手段を含むことを特徴とする無線携帯端末システム。

【請求項 2】 前記無線通信手段は前記金融機関のセンター端末と無線で接続される無線携帯端末と、この無線携帯端末に挿入されるカードとからなり、このカードは前記金融機関のセンター端末より引き落とされる金銭情報の加算および前記金融機関のセンター端末に預け入れされる金銭情報の減算が行われる演算手段と、この演算手段で演算後の残高が格納される格納手段とを有することを特徴とする請求項 1 記載の無線携帯端末システム。

【請求項 3】 前記カードは前記暗証番号の確認を行う確認手段をさらに有することを特徴とする請求項 2 記載の無線携帯端末システム。

【請求項 4】 前記暗証番号は前記無線携帯端末より入力され前記カードに送られることを特徴とする請求項 2 または 3 記載の無線携帯端末システム。

【請求項 5】 前記暗証番号は金銭情報の保護用と金融機関アクセス情報の保護用の 2 種からなることを特徴とする請求項 1 ～ 4 いずれかに記載の無線携帯端末システム。

【請求項 6】 前記無線携帯端末は第 1 の鍵を有し、この第 1 の鍵により金銭情報を暗号化して前記カード内の格納手段に格納する暗号化手段をさらに有することを特徴とする請求項 2 ～ 5 いずれかに記載の無線携帯端末システム。

【請求項 7】 前記無線携帯端末は第 2 の鍵を有し、この第 2 の鍵により前記暗号化された金銭情報を復号化して読み出す復号化手段をさらに有することを特徴とする請求項 6 記載の無線携帯端末システム。

【請求項 8】 前記カードは前記無線携帯端末より第 2 の鍵を受取り、前記暗号化された金銭情報を復号化して読み出す第 2 の復号化手段をさらに有することを特徴とする請求項 6 記載の無線携帯端末システム。

【請求項 9】 前記無線携帯端末は、前記カードに電源を供給する電源供給手段を有することを特徴とする請求項 2 ～ 8 いずれかに記載の無線携帯端末システム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】 本発明は無線携帯端末システムに関し、とくに IC カードにより金融機関と金銭の授受を行う無線携帯端末システムに関する。

【0002】

【従来の技術】 IC カードにより金融機関と金銭の授受を行う、いわゆる電子財布システムは知られている。

【0003】 この電子財布システムは、銀行、各種金融機関が顧客に予め IC カードを発行しておき、顧客が買物をする際、ATM（現金自動支払機）より、現金の代

わりに金銭データを IC カードに書き込み、顧客は店で買物した金額をこの IC カードにより支払うシステムである。

【0004】 この電子財布システムは、顧客が現金を持ち歩く必要がない点、および店から銀行に売上金を運搬する現金輸送車が不要である点等から安全性が高く、効率的である。

【0005】 また、たとえばプリペイドカード（料金先払いカード）の場合であれば、予め表示された金額を使い果たすとそのカードでさらに買物をすることはできなかったが、電子財布システムでは IC カードに記憶された金額がゼロとなっても、その IC カードに設けられたテンキーにより新たに必要な金額を追加することで、さらに買物をするができる。もっとも、その追加する金額が自己の口座に存在することが前提となるのはいうまでもない。

【0006】 このような電子財布システムの一例が特開平 3 - 9 2 9 6 6 号公報および特開平 5 - 9 4 4 5 8 号公報に開示されている。

【0007】 特開平 3 - 9 2 9 6 6 号公報に開示された技術は、IC カードに表示部と入力キーとを持たせ、小型のコンピュータの機能を持たせながら、IC カードを使用する際はこの IC カードに電源を入れ、パスワードを入力してから現金の引き落とし、またはプリペイドカード機能を使用するものであり、特開平 5 - 9 4 4 5 8 号公報に開示された技術は、IC カードおよび店舗取引端末で構成される電子財布システムにおいて、その認証手段に必要な銀行鍵を個人ごとにユニークにし、さらにこれを時間可変な鍵とするものである。

【0008】

【発明が解決しようとする課題】 しかし、従来の電子財布システムは、まず第 1 に IC カードに金銭をチャージする（金額を書き込む）場所および時間が限定されるという欠点がある。

【0009】 これは、金銭をチャージする場所は各金融機関に設置されている ATM（Automatic Teller Machine；現金自動預金払出機）に限定されるということである。

【0010】 第 2 に IC カードを紛失したり盗難されたりすると、第三者に IC カードの情報を盗まれる可能性が大きくなるという欠点がある。

【0011】 これは、従来の IC カードは暗証番号および金額を入力するための入力キーおよび金額の表示部を備えているため、このキー入力により暗証番号が一致すれば金銭の使用が可能となるためである。

【0012】 第 3 に IC カードの使用方法が複雑であるという欠点がある。

【0013】 これは、銀行などの ATM から金銭をチャージする場合は、この IC カードの入力キーで暗証番号を打ち込み、IC カードを起動させてから ATM のカー

ド差し込み口に挿入し、さらにATMの暗証番号を打ち込むという二重の操作を行わなければならないことである。また、このICカードをプライベートカード代わりに店舗で使用する場合も、まずカードの電源を入れ、次にICカードに暗証番号を打ち込んでICカードを稼働状態にしてから使用するという手順を踏まなければならないことである。

【0014】第4にICカードが電池切れになるとICカードの使用ができなくなるという欠点がある。

【0015】これは、ICカードを起動ためには電池が必要だからである。当然ながら電池がなくなりICカードを起動することができなければ、金銭をICカードにチャージできないばかりか、ICカードにチャージされた金銭を使用することさえできなくなる。

【0016】そこで本発明の目的は、金銭をチャージする場所が限定されず、ICカードを紛失等しても第三者にICカードの情報を盗まれる可能性が少なく、ICカードの使用方法が容易で、かつICカードの電池切れという事態を回避することができる無線携帯端末システムを提供することにある。

【0017】

【課題を解決するための手段】前記課題を解決するために本発明は、金融機関のセンター端末と無線で接続され、金銭情報のやりとりと暗証番号の確認を行うことで金銭情報の引き落としおよび預け入れを行う無線通信手段を含むことを特徴とする。

【0018】

【発明の実施の形態】本発明によれば、金融機関のセンター端末と顧客の携帯端末とを無線で接続し、金融機関の自己の口座より金銭を携帯端末にチャージする。

【0019】以下、本発明の実施例について添付図面を参照しながら説明する。図1は本発明に係る無線携帯端末システムの構成図である。

【0020】無線携帯端末システムは、無線携帯端末1と、この無線携帯端末1に挿入されるICカード2とからなり、この無線携帯端末1の通信は中継局3を経由して金融機関4のセンター端末5および店舗6のレジ端末7と無線で行われる。

【0021】金融機関4には各顧客の金銭情報が管理されている。顧客はまず無線携帯端末1にICカード2を挿入し、無線携帯端末1上の入力キーより必要な金銭を打ち込む。するとこの情報は中継局3およびセンター端末5を経由して金融機関4に入力される。そして、その必要な金銭が金融機関4のその顧客の口座から差し引きされ、次いで顧客のICカード2にその金銭がチャージされる。

【0022】顧客が店舗6で買物する場合は、そのICカード2をその店舗2に持参し、そのICカード2を店舗6内のレジ端末7に挿入すると、買物した金銭がそのICカードから差し引かれる。店舗6はそのICカード

2から読み出した顧客情報をもとにレジ端末7、中継局3およびセンター端末5を経由して金融機関4に対し金銭の支払いを請求する。これに対し、金融機関4は先にICカード用として差し引かれた顧客の金銭から必要な金銭を店舗6の口座に振り込む。

【0023】次に、無線携帯端末1の構成について説明する。図2は無線携帯端末の一実施例の構成図である。

【0024】無線携帯端末1は、CPU（中央処理演算ユニット）11と、クロックジェネレータ12と、バスコントローラ13と、DMA（Dynamic Memory Access）コントローラ14と、マスクROM15と、フラッシュメモリ16と、DRAM（ダイナミックRAM）17と、LCD（液晶表示器）18と、タッチパネル19と、PWM（音声）出力20と、無線部21と、メモリインタフェース22と、LCDインタフェース23と、I/Oインタフェース24と、無線部インタフェース25と、ICカード用電源26とからなる。

【0025】CPU11は、本発明である無線携帯端末1のソフトウェアを実行するための心臓部であり、本無線携帯端末1のOSおよびアプリケーションプログラムを実行する部分である。OS部はマルチタスク方式になっており、各電子決済プログラム等のアプリケーションソフトの実行と無線のプロトコル、タッチパネル19の補正等の処理を時分割で実行する。

【0026】クロックジェネレータ12はクロック発生部である。

【0027】バスコントローラ13は、CPU11とメモリインタフェース22、CPU11とLCDインタフェース23、CPU11とI/Oインタフェース24、CPU11と無線部インタフェース25、DMA14による転送を主体としたメモリインタフェース22とLCDインタフェース23、メモリインタフェース22とI/Oインタフェース24、メモリインタフェース22と無線部インタフェース25夫々の間のデータ転送についてアービトレーション（調停）を行う。

【0028】DMA14は各メモリ15～17とLCD18、各インタフェース22～25、無線間のデータをCPU11がメインバスにアクセスしていない空き時間にデータを自動で転送する。

【0029】マスクROM15は、無線携帯端末のOSや基本アプリケーションを格納するためのROMである。

【0030】フラッシュメモリ16には、本システムのOS、無線のプロトコルを実行するためのドライバ、財布の機能を実現するための金銭管理プログラム、金銭情報・店名番号・口座番号・暗証番号等の暗号化・復号化プログラム、ICカード2のリード・ライト用のプロトコルを実行するためのドライバ、タッチパネル19のドライバ、音声コーデックのドライバが基本プログラムと

して内蔵される。

【0031】DRAM17は、主にアプリケーションのワーク、LCD18のVRAM（ビデオRAM）、I/Oに接続される周辺ブロックのワーク、無線部インタフェース25の受信データの保存用として使用される。

【0032】LCD18は、本無線携帯端末システムの表示媒体であり、金融機関4へアクセスを行う際のガイド情報、金銭情報を引き出す際に使用する暗礁番号の書き換え画面等を表示する。

【0033】タッチパネル19は、本無線携帯端末システムの入力手段であり、LCD表示画面の上に載せて使用し、LCD18の表示位置とタッチパネル19の入力位置をリンクさせてLCD18上に表示された疑似的なタイプライタやテンキー、ボタン等を押すとその応答をLCD18に表示させ、押されたことを確認できるような形にする。

【0034】PWM出力20は、音声を出力する部分であり、前述した金融機関4へアクセスを行う際に画面情報と併せて音声ガイドを行う。

【0035】無線部21は、本システムの通信手段である。無線、たとえばPager（ポケットベル）等の電波は構造上ビルの中でも突き抜けて使用できるため、無線を使用することでどここの場所にいても金銭を引き出すことができる。

【0036】メモリインタフェース22は、マスクROMや、追加アプリケーションやICカード2のバックアップ情報を格納するためのフラッシュメモリ16とワークエリアや無線携帯端末の受信データを格納するためのDRAM17にアクセスするためのインタフェース機能を持つ。

【0037】LCDインタフェース23は、LCD18とCPU11、DMA14間の信号のやりとりを中継する。DRAM17上のバッファに蓄えられたLCD18の表示データはDMA14を使用してLCD18に転送されるが、LCDインタフェース23はDRAM17に書き込まれた階層情報を含んだLCDデータをLCD18の表示データに変換する機能を併せ持つ。

【0038】I/Oインタフェース24には、金銭情報を書き込むためのICカード2、手書きデータを入力したりデータの選択を行ったりするための入力手段であるタッチパネル19、ユーザインタフェースとして応答に使用する音声出力20が接続される。

【0039】無線部インタフェース25は、中継局3と無線携帯端末1間のデータをやりとりするための通信回路である無線部21とのインタフェースおよび無線部レジスタとのインタフェースを受け持つ。

【0040】ICカード用電源26はICカード2に電源を供給するためのものである。

【0041】なお、このI/Oインタフェース24と接続されるICカード2は、後述するが内部にメモリを備

えたクレジットカードサイズのメモリであるが、本システムではこのICカード2にCPUも搭載することでICカード2をインテリジェント化させ、任意の入力データに対し演算処理を施して外部に結果を返せるようにする。

【0042】次に各インタフェースの構成について説明する。図3はバスコントローラ13の構成図である。バスコントローラ13は、DRAMリフレッシュジェネレータ31と、アービター（調停部）32と、アドレスデコーダ33とからなる。

【0043】DRAMリフレッシュジェネレータ31は、DRAM17に対してメモリのリフレッシュを行うための信号を作り出すためのタイミングをカウントし、アービター32に対しリフレッシュの要求を行う部分である。

【0044】アービター32は、CPU11とメモリ間等、各インタフェース22～25のデータバスがぶつからないようにアービトレーション（調停）を行う部分である。夫々のインタフェース22～25には優先順位を付けて夫々のインタフェースからバスのアクセス要求が来たときに優先順位の高いものから順番にバスを開放する役目を担う。

【0045】アドレスデコーダ33は、前もって決めておいた各インタフェース22～25のアドレス領域をCPU11がアクセスしたときの選択信号を生成する部分である。

【0046】なお、同図に示す入出力信号は信号名および行き先のみを示し、動作説明は省略する。以下、図7まで同様である。

【0047】図4はメモリインタフェース22の構成図である。メモリインタフェース22は、DRAMアドレスジェネレータ41と、フラッシュアドレスジェネレータ42と、Dバスサイジング43と、RDYシグナルジェネレータ44と、リフレッシュシグナルジェネレータ45と、RAS・CASジェネレータ46とからなる。

【0048】DRAMアドレスジェネレータ41は、CPU11がDRAM17にアクセスを行うときのCPU11のアドレスをDRAM17用のRAS・CASアドレスに変換する部分である。

【0049】フラッシュアドレスジェネレータ42は、CPU11がフラッシュメモリ16にアクセスを行うときのCPU11のアドレスをフラッシュメモリ16のアドレスに変換する部分である。フラッシュメモリ16のアクセス方式は、DRAM17のようにRAS・CASでアクセスする方式や、フルアドレスでアクセスする方式があるので使用するメモリの種類によって対応させる必要がある。

【0050】Dバスサイジング43は、CPU11のデータバスのビット幅を各メモリ用のビット幅に変換する部分である。

【0051】たとえば、CPU11のビット幅が16ビットで、メモリのビット幅が8ビットのとき、CPU11の16ビット幅のデータを上位8ビットと下位8ビットの2回に分けてメモリに書き込むようにする。

【0052】RDYシグナルジェネレータ44は、バスコントローラ13からのIF・ADS信号に対してのRDY (READY) 信号を生成する部分である。

【0053】リフレッシュシグナルジェネレータ45は、バスコントローラ13のリフレッシュ信号をトリガとして、夫々のDRAM17ごとのリフレッシュタイミングに合わせてRAS・CASを合成する部分である。

【0054】RAS・CASジェネレータ46は、DRAM17に対してのアクセス信号、およびリフレッシュ信号を生成する部分である。

【0055】図5はLCDインタフェース23の構成図である。LCDインタフェース23は、コントロールシグナルジェネレータ51と、バスサイジング52と、フィールド53と、セクタ54とからなる。

【0056】コントロールシグナルジェネレータ51は、表示媒体であるLCD18のコントロール信号を生成する部分であり、LCD18のフレーム番号、ラインデータロード信号、LCD駆動電圧交流化信号、シフトレジスタのクロックパルス信号等が含まれる。

【0057】図6はI/Oインタフェース24の構成図である。I/Oインタフェース24は、アドレスデコーダ61と、コントロールシグナルジェネレータ62と、セクタ63、64とからなる。

【0058】アドレスデコーダ61は、I/OへのアクセスがICカード2であるか、音声出力20であるか、タッチパネル19であるかをセレクトする信号とI/O部のレジスタをセレクトする信号を生成する部分である。

【0059】コントロールシグナルジェネレータ62は、ICカード2、音声出力20、タッチパネル19に対する制御信号を生成する部分で、たとえばICカード2に対してはクロックやリセット信号等を生成する。

【0060】セクタ63、64は、各データの入出力の方向を選択するものである。

【0061】図7は無線部インタフェース25の構成図である。無線部インタフェース25は、アドレスデコーダ71と、バスサイジング72と、コントロールシグナルジェネレータ73とからなる。

【0062】アドレスデコーダ71は、無線部21のレジスタをセレクトするための信号を生成する。

【0063】バスサイジング72は、CPU11のデータバスのビット幅を無線データのビット幅に変換する部分である。

【0064】コントロールシグナルジェネレータ73は、無線部21のコントロール信号を生成する部分である。

【0065】次に、ICカード2の構成について説明する。図8はICカード2の構成図である。

【0066】ICカード2は、CPU81と、メモリインタフェース82と、メモリMem1、Mem2と、シリアルインタフェース83と、シリアルI/O84とからなる。

【0067】CPU81は、ICカード2の演算処理部で暗証番号の確認、その他金銭の加算・減算等の処理を行う。

【0068】メモリMem1、Mem2はCPU11の実行するプログラムの格納や実行時のワークエリアとして使用する。

【0069】メモリインタフェース82はこれらのメモリとCPU11間のインタフェースフェースを取り持つ。

【0070】このようにメモリ領域をMem1とMem2とに分けたのは、セキュリティを強化するためである。すなわち、外部にシリアルI/O85を介して出力するデータはMem2の領域のみを見せて、Mem1の領域はICカード2の暗証番号を入れない限り、無意味なデータしか読めず、書き込みは不可能とする機能をこのICカード2に持たせる。

【0071】シリアルI/O84は、ICカード2のデータの入出力部である。ICカード2はこの部分を通してID情報や金銭情報等の各種データを出し入れする。

【0072】シリアルインタフェース83は、このI/O84とCPU81間のインタフェースを取り持つ。

【0073】次に、ICカード2の動作について説明する。まず第1に、ICカード2に保存する情報であるが、ICカード2にはカードが本人のものであることを確認するためのID情報と金融機関にアクセスするための暗証番号を書き込む。この情報はICカード2のMem1に格納しておく。

【0074】ID情報の中身はICカードが提携している金融機関の銀行番号、店番号、科目、口座番号、顧客の名前等であり、暗証番号の中身は無線携帯端末1を使用して金融機関との現金授受プログラムを起動させるための暗証番号Aと、各金融機関ごとの暗証番号Bの2種類を持たせる。

【0075】ここで、暗証番号Aは顧客が無線携帯端末1を扱いICカード2のID情報を確認したり、金融機関にアクセスするための前処理のための暗証番号であるため、この暗証番号は顧客が後から書き換えられるものとする。

【0076】一方、暗証番号Bは各金融機関ごとに固有のものであるため、顧客が提携している銀行が複数あれば、複数の暗証番号が必要となる。また、この暗証番号Bは金融機関と契約された暗証番号であるため、顧客側では勝手に書き換えることはできない。

【0077】また、本システムに使用するICカード2

は、いわゆるプリペイドカードと同様な機能も持たせる必要があるため、ICカード2内に蓄えられている金銭情報は第三者にも確認できる必要がある。その反面、個人情報、ID情報、暗証番号等、他人には知られたくないデータも同時にこのICカード2に書き込む必要がある。

【0078】そこで、前述したMem2に金銭情報を格納し、Mem1に個人情報、ID情報、暗証番号等を格納する。これにより、第三者は金銭情報は読み出せるが、個人情報、ID情報、暗証番号等は読み出せないことになる。

【0079】図9はICカードの読み書き制御を示すフローチャートである。外部からシリアルI/O84を介して入力されたコマンドをCPU81が解析し、そのコマンドに対する応答結果を再びシリアルI/O84を介して外部に返すという形式をとる。

【0080】まず、外部よりメモリリードのコマンドがICカード2に入力されると(S1)、CPU81はMem1のマスクが解除されているかを調べる(S2)。

【0081】後述するが、暗証番号Aが確認されていないとこのマスクは解除されない。したがって、第三者が入力したコマンドであればMem1のマスクは解除されていないので、CPU81は外部にダミーデータ(でたらめなデータ)を出力する(S3)。一方、顧客が入力したコマンドであればMem1のマスクは解除されているので、正規データが出力される(S4)。

【0082】同様に、外部よりメモリライトのコマンドがICカード2に入力されると(S5)、CPU81はMem1のマスクが解除されているかを調べる(S6)。第三者が入力したコマンドであればMem1のマスクは解除されていないので、CPU81はライトコマンドを無視する(S7)。一方、顧客が入力したメモリライトのコマンドであればMem1のマスクは解除されているので、正規データが出力される(S8)。

【0083】外部より暗証番号A相当のデータがICカード2に入力されると、CPU81は暗証番号Aかどうかを確認する(S10)、そして暗証番号Aと確認するとマスクを解除する(S11)。一方、暗証番号Aと確認しなければエラーコードを出力する(S12)。

【0084】外部より暗証番号B相当のデータがICカード2に入力されると、CPU81は暗証番号Bかどうかを確認する(S15)、そして暗証番号Bと確認するとマスクが解除されているかを確認する(S16)。もし、顧客であれば、後述するがまず暗証番号Aを入力しているはずであり、この場合はマスクは解除されている。したがって、マスクは解除されているので金融機関へのアクセスが可能となる(S17)。一方、暗証番号Bと仮に(偶然に)確認された場合であっても、これが第三者によるものであれば、暗証番号Aは確認されていないはずであるから、マスクは解除されていない。した

がって、この場合はエラーコードを出力する(S18)。また、S15に戻り、S15で暗証番号Bが確認されない場合はエラーコードを出力する(S18)。

【0085】図10は金銭授受プログラムを起動させる手順を示すフローチャートである。図10において暗証番号Aを入力する手順は本無線携帯端末1に接続されるICカード2のID情報を読み書きできるモードに移行させるための手段である。このモードはICカード2の所有者がID情報を確認する場合にも適用される。これを行うことで第三者にカードの中身を知られないようにする。

【0086】暗証番号Bを入力する手順は金融機関4に預けている預金を引き出したり預けたりする場合に使用する。

【0087】この場合も暗証番号の処理はICカード2内部で行うようにし、電波に乗せて外部に情報が漏れることのないようにする。

【0088】暗証番号Aは顧客が所定のプログラムで自由に書き換えられるようにし、暗証番号BはICカード2を発行する際に金融機関4側で書き込み、顧客は自由に書き換えはできないようにする。

【0089】この場合の所定のプログラムとは無線携帯端末1側に入っている。但し、ICカード2内に記載されている暗証番号Aの書き換えは、前回設定された番号をICカード2が確認したときのみ行えるようにし、この書き換えを実際に行うのはICカード2であることはいうまでもない。

【0090】次に、フローの詳細について説明する。同図の左側が無線携帯端末1のフロー、右側がICカード2のフローである。

【0091】まず、無線携帯端末1へICカード2を挿入し、無線携帯端末1のタッチパネルより暗証番号Aを入力すると、無線携帯端末1よりICカード2へリクエスト信号が送出される(S21)。これに対し、ICカード2より確認(Ack)信号が返送される(S22)。この確認信号を受けると、無線携帯端末1よりICカード2へ暗証番号Aが送信され、暗証番号A確認のプログラムが起動する(S23)。

【0092】すると、ICカード2は暗証番号Aの確認を行い、本人のものと確認されない場合は異常終了を示すエラーコードを無線携帯端末1へ返送し(S24)、動作を終了させる(S25)。

【0093】一方、暗証番号Aが本人のものと確認された場合は正常確認コードを無線携帯端末1へ返送し(S26)、正常終了させる(S27)。これにより、ICカード2のシークレットエリアは解除される(S28)。すなわち、Mem1の内容の読み出し、書き込みが可能となる。これで、金融機関4との通信が確立する(S29)。

【0094】金融機関4との通信が確立すると、無線携

帯端末1のタッチパネルより暗証番号Bを入力する。すると、無線携帯端末1よりICカード2へリクエスト信号が送出される(S30)。このリクエスト信号を受けると、ICカード2は暗証番号B確認のプログラムを起動し(S23)、無線携帯端末1へ確認信号を返送する(S32)。

【0095】この確認信号が無線携帯端末1で受信されると、無線携帯端末1より暗証番号BがICカード2に送信される(S33)。次に、ICカード2では暗証番号Bの確認が行われ(S34)、金融機関4が本人のものと確認されると正常確認コードが無線携帯端末1に返送される(S35)。

【0096】一方、本人のものと確認されない場合は、異常終了を示すエラーコードが無線携帯端末1に返送される(S36)。なお、異常終了の場合は3回まで暗証番号Bの再入力認められるが(S37)、3回入力しても異常終了となる場合はICカード2は動作を異常終了させる(S38)。そして、この場合、無線携帯端末1より金融機関4に対し、このICカード2の不正使用の情報が送信される(S39)。

【0097】正常確認コードが無線携帯端末1に返送されると、無線携帯端末1よりICカード2に対する金銭の入出力が可能となる(S40)。すると、無線携帯端末1よりICカード2に対しカード残高書き換え要求信号が送信され、これに対する確認信号が無線携帯端末1に返送されると(S42)、ICカード2では残高の書き換えが行われる(S43)。

【0098】残高の書き換えが終了すると、無線携帯端末1よりICカード2に対しシークレットエリア起動要求信号が送信され(S44)、これを受信したICカード2は確認信号を返送する(S45)。そして、ICカード2のMem1は再び読み出し書き込みができなくなる。

【0099】次に、ICカード2の金銭情報の変更が無線携帯端末1より金融機関4へ送信され、動作は終了する。

【0100】尚、ID情報等のICカード2のデータを無線携帯端末1側に読み込むためには秘密鍵を使用する必要がある。秘密鍵は後で述べる暗証番号Bを利用する。

【0101】まず、ICカード2のシークレットエリアを開放するための暗証番号AをICカード2に転送してICカード2のシークレットエリアであるID領域を開放する。これによりICカード2による預金引き出し可能状態となる。

【0102】次に金融機関4にアクセスするための暗証番号Bを入力する。無線携帯端末1は暗証番号BをICカード2に転送し、ICカード2は暗証番号Bを受け取ったら、これを秘密鍵として公開鍵と併せて内部データの暗証番号Bの復号化を行う。

【0103】次に復号化された暗証番号Bと入力された暗証番号Bが一致するかどうか確認し、一致したら図10の引き出しまたは預金金額の入力プロセスに移行する。

【0104】預金取引終了後、ICカード2内の暗証番号Bによる復号化の際のバッファは全て消去する。また、無線携帯端末1側はICカード2の切断が確認され次第、内部バッファにためられている暗証番号Bに関するバッファを全て消去する。これはICカード2アクセス中に無理矢理、無線携帯端末1とICカード2との接続を切られた場合にも適用する。

【0105】このICカード2をプリペイドカードとして使用するとき、先に述べたとおり第三者がICカード2の金銭情報を読み書きできなければならない。

【0106】このとき、第三者またはこのカード2の持ち主が金銭情報を勝手に書き換えて金額を増やすといったことはできないようにする必要がある。

【0107】その方法を図11に示す。図11は金銭情報書き換えのプロテクトの手順を示すフローチャートである。

【0108】金銭の加算(S51)については無線携帯端末1が金融機関4との接続を行っていることを確認し(S52)、接続できているときは、加算金額分だけICカード2に加算するようにし(S53)、接続ができていないときは、ICカード2はエラーコードを返してコマンド待ちに戻るようにしておく(S54)。この接続の確認は、暗証番号A、暗証番号Bの入力が確認され、更に金融機関4からの接続OKのコードを無線携帯端末1から受け取ったときにICカード2は接続OKフラグを立てる。このフラグが立っているときは前回の金銭に加算金額分だけ値を増やす。

【0109】金銭の減算(S56)についてはこの確認は行わず、減算金額分だけ前回の金額から値を減らす(S57)。

【0110】また、ICカード2内のデータは全て暗号化しておく。暗号化にはDES(Data Encryption Standard)やFEAL(高速データ暗号化処理手順)などの共通鍵の方式を取ることもできるし、更に安全性を確保するにはRSA(暗号化方式の一種)などの公開鍵の方式を取ることも考えられる。

【0111】暗号化を行うにはまず暗号化の鍵となる物が必要になる。また暗号化されたデータを復号化するための鍵がなければデータを復号できない。

【0112】共通鍵の方式とはこの暗号化と復号化の鍵を同一にする方式である。一方、公開鍵の方式とは暗号化を行うには鍵Aのみで行えるが復号化を行うには鍵Aと鍵Bを必要とする方式である。鍵Aは鍵Bから生成される鍵で鍵Aからは鍵Bは合成できない。この鍵Aを公開鍵と予備鍵Bを秘密鍵と呼んでいる。

【0113】例として図12に公開鍵の方式でICカー

ド2のデータに暗号化をかけた例を示す。図12は暗号化及び復号化の手順のフローチャートである。まず、同図(A)の暗号化について説明する。

【0114】携帯無線端末1上に蓄えられているデータまたはICカード2から読み取ったデータを平文とし暗号をかけるための鍵を公開鍵、公開鍵によって暗号化されたデータを暗号文とする。ICカード2のデータは他人に容易には読めないように暗号化をして保存をしておく必要がある。

【0115】この暗号化をICカード2より処理能力の大きい無線携帯端末1側で行う。まず暗号化されていない平文を先に述べた公開鍵により、暗号化する(S81)。暗号化の終了した暗号文は随時ICカード2側に送信する(S82)。この様にすることで、たとえばカード2を何らかの手段で手に入れた自分以外の者が中身のデータを読み込めたとしても暗号化されたデータが入っているだけで、他の者には復号化しない限り意味のあるデータにならないため悪用されることはない。

【0116】一方、復号時のパターンとしてはA、Bの2種類が考えられる。まず復号時同図(B)について説明を行う。同図(B)はICカード2内に公開鍵を予め書き込んでおいて復号化をICカード2内で行う方式である。復号時は顧客が無線携帯端末1の入力手段から秘密鍵を打ち込み(S61)、その鍵をICカード2に転送し(S62)、ICカード2は無線携帯端末1から受け取った秘密鍵と予め書き込まれている公開鍵を利用してICカード2内に書き込まれている暗号文を復号化し(S63)、無線携帯端末1に復号化された後の平文を転送する(S64)。

【0117】この様にすると復号化の処理がICカード2内で完結するため、他の端末から暗号化されたデータを読み出す事もBの方式に比べ容易にできる。

【0118】次に復号時同図(C)について説明を行う。同図(C)はICカード2内の暗号化されたデータをICカード2に比べ処理能力の高い無線携帯端末1側で復号化することができる。

【0119】暗号化されたデータを復号化するには、まず無線携帯端末1はICカード2に内部の暗号文を転送してもらう(S71)。データの読み込みが終了したら、入力手段により無線携帯端末1に秘密鍵を打ち込む(S72)。無線携帯端末1は、この秘密鍵と予め書き込まれている公開鍵を使用して、先にICカード2から読み取った暗号文を復号化する。

【0120】この方法の時に他の端末でICカード2の内容を読む場合には、赤外線等の無線またはRS-232Cなどの有線によって他の端末に公開鍵を転送した後復号化を行うということが考えられる。

【0121】次に図12で使用する公開鍵の作成の手段及びその使用方法例、また秘密鍵の作成手段及びその使用方法例を示す。

【0122】公開鍵は金融機関4毎の暗証番号B(これを秘密鍵にする)とICカード2のシリアルナンバーから生成する。金融機関4は、まず最初にICカード2へID情報、暗証番号Bの登録を行う必要があるのとICカード2を発行する側なのでシリアルナンバーは当然知っている。ゆえに公開鍵の生成は金融機関4側で行う。金融機関4は公開鍵生成後、公開鍵により暗号化されたID情報と平文の公開鍵をICカード2に書き込みを行い、その後ICカード2を顧客に送る。

【0123】このときID情報は図8のMem1に書き込む必要があり、ここにアクセスするために暗証番号Aを必要とする。暗証番号Aは顧客が自由に書き換え可能な番号であるが、ICカード2を発行する際のデフォルト(省略)では暗証番号を入力しないでおく。そうすれば、顧客は最初にICカード2のID情報を見る時には暗証番号を入力することなしにID情報にアクセスすることができる。

【0124】顧客はICカード2を受け取ったら、まず最初に無線携帯端末1とICカード2を接続し無線携帯端末1に公開鍵の設定を行う。無線携帯端末1側はICカード2が接続されたのを確認した後、公開鍵のデータ引き渡し要求をICカード2に送る。ICカード2は要求を受け取ったら、無線携帯端末1側に公開鍵を転送する。無線携帯端末1側は公開鍵を受け取ったら内部のメモリに公開鍵の情報をバックアップする。これで無線携帯端末1側の初期設定は終了である。無線携帯端末1側は次回よりICカード2にデータを書き込む際はこの公開鍵を基に暗号化を行った上で行う。

【0125】ICカード2を使用して店舗6などで品物を購入する際は、店舗6側が予め金融機関4とICカード2の使用契約をしておく。この際にICカード2のID情報を読み出すための種別コードを金融機関4からもらう。この種別コードを店舗6側が持っているICカード2専用のレジ端末7に登録しておく。

【0126】レジ端末7はICカード2が接続されたら自分の種別コードをICカード2に転送する。ICカード2はレジ端末7の種別コードを受け取ったら、ID領域を開放し金銭情報を引き出せる状態に移行する。

【0127】チャージされている金銭を取り出すときはICカード2に金銭の取り出し要求を発行し、ICカード2は要求された金額分だけチャージされた金銭を減らし内部メモリMem2の金銭情報を書き換える。書き換えが正常に終了したらACKを返す。要求金額が残金より大きいなどで書き換えが正常に行えない場合は、異常終了コード及びエラーコードを返し内部メモリの金銭情報の書き換えは行わない。

【0128】レジ端末7側は前もってICカード2にチャージされている残金分かっているので、取り出す金額がICカード2の残金よりも大きい場合は残金分だけの要求をICカード2に行う。

【0129】また、銀行などで現金を引き出す場合はATM側が出力する自分の種別コードをICカード2側に送ることで、ICカード2は内部のシークレット領域をID情報の領域のみ開放しATMからID情報を読み出せるようにする。また、ATMにより現金を引き出すときは図10で示した暗証番号Bを利用して金銭をICカード2にチャージするのと同様な方法で現金を引き出せるようにする。

【0130】但し、ICカード2への金銭チャージは暗証番号Aを入力して、ICカード2の全領域を開放しないといけないようにしておく。

【0131】また本発明に使用する無線通信は双方向に通信できる手段であればPager（ポケットベル）以外のPHS（Personal Handyphone System）やセルラーなどの方式でも構わないし、ICカード2についても内部にCPUを内蔵できる機構であればPCMCSA（Personal Computer Memory Card Standard Association）などのカードでも問題ない。

【0132】また、無線携帯端末1内にICカード2に電源を供給するための電源26を備えたので、ICカード2用の電池は不要となる。

【0133】

【発明の効果】本発明によれば、第1に金融機関のセンター端末と無線で接続され、金銭情報のやりとりと暗証番号の確認を行うことで金銭情報の引き落としおよび預け入れを行う無線通信手段を含み携帯端末システムを構成したので、金銭情報の引き落としおよび預け入れをATMのない場所でも行うことができる。また、時間が限定されるということもない。

【0134】第2にICカードに入力キー、表示部を備えないため、第三者に暗証番号を不正に入力されるおそれがない。また、仮になんらかの方法で暗証番号が入力され、内部の金銭情報が読み出されたとしても金銭情報は予め暗号化されているため、容易に読み出すことは困難である。

【0135】第3に、暗証番号の入力は無線携帯端末に

対して行うだけで済むので使用方法が簡易となる。また、ICカードを店舗で使用する場合でも店舗のレジ端末に対する操作のみで済むため使用方法が簡易となる。

【0136】第4に、ICカードの電源供給は無線携帯端末より行うため、ICカードの電池が不要となる。したがって、電池切れで使用不可能という事態を回避することができる。また、ICカード2のみでは作動しないため不正使用の防止にもなる。

【図面の簡単な説明】

【図1】本発明に係る無線携帯端末システムの構成図である。

【図2】同システムの無線携帯端末の一実施例の構成図である。

【図3】同システムのバスコントローラの構成図である。

【図4】同システムのメモリインタフェースの構成図である。

【図5】同システムのLCDインタフェースの構成図である。

【図6】同システムのI/Oインタフェースの構成図である。

【図7】同システムの無線部インタフェースの構成図である。

【図8】同システムのICカードの構成図である。

【図9】同システムのICカードの読み書き制御を示すフローチャートである。

【図10】同システムの金銭授受プログラムを起動させる手順を示すフローチャートである。

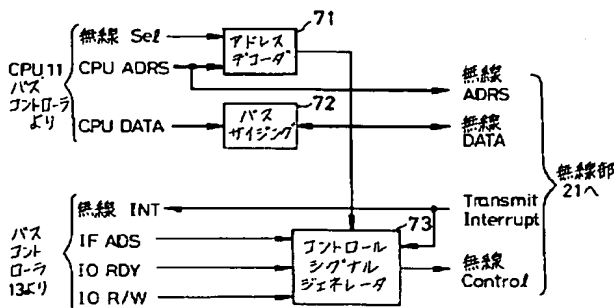
【図11】同システムの金銭情報書き換えプロテクトの手順を示すフローチャートである。

【図12】同システムの暗号化および復号化の手順を示すフローチャートである。

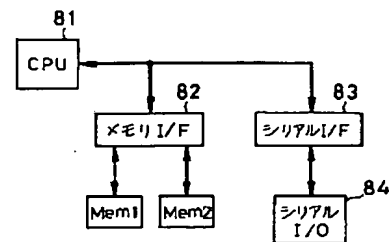
【符号の説明】

- 1 無線携帯端末
- 2 ICカード
- 4 金融機関
- 5 センター端末
- 26 電源

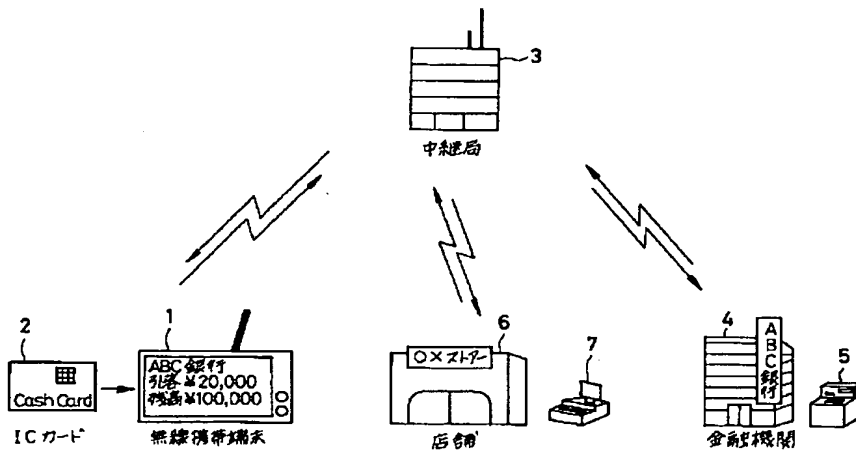
【図7】



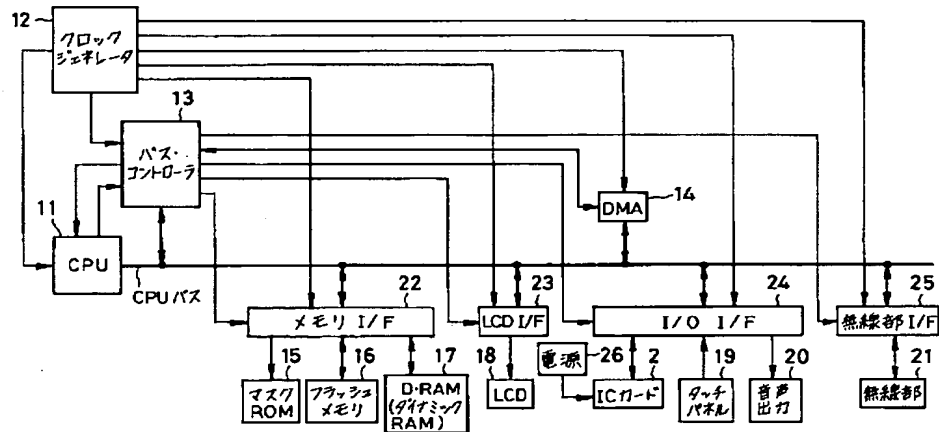
【図8】



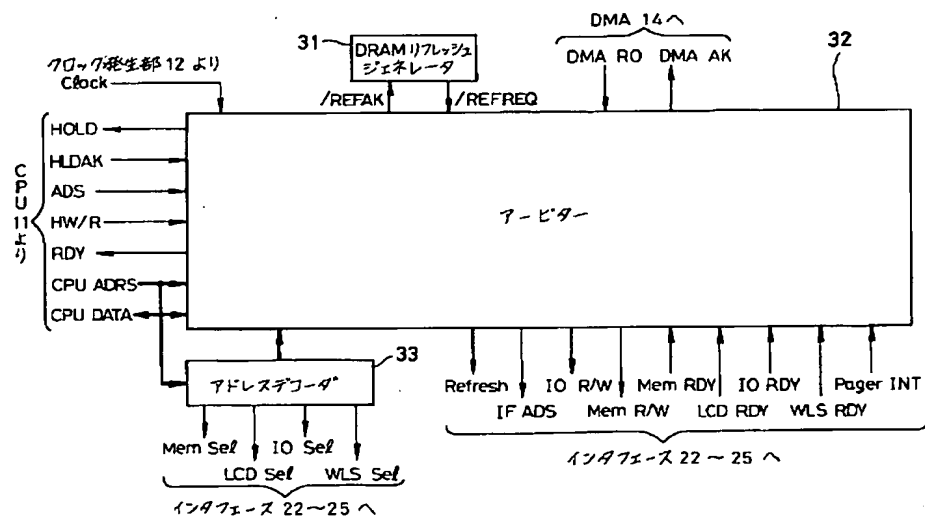
【図 1】



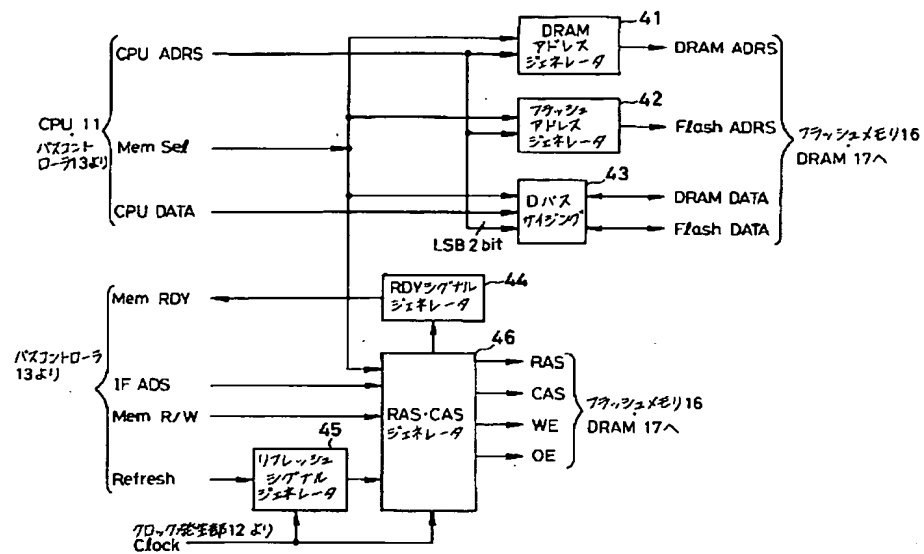
【図 2】



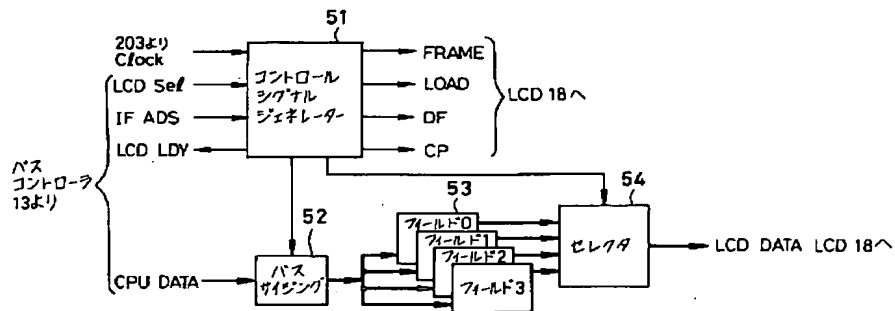
【図 3】



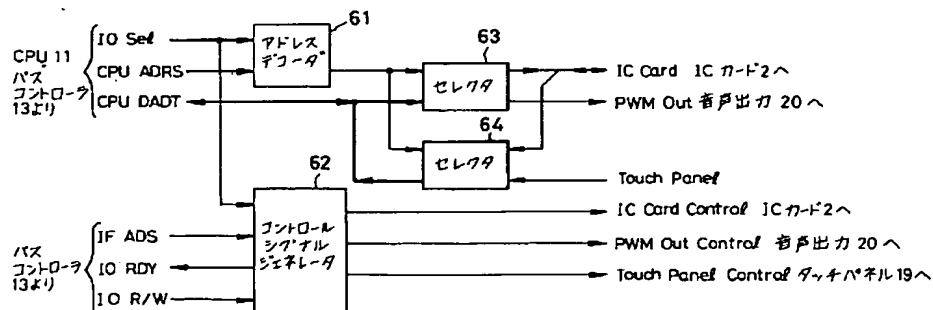
【図 4】



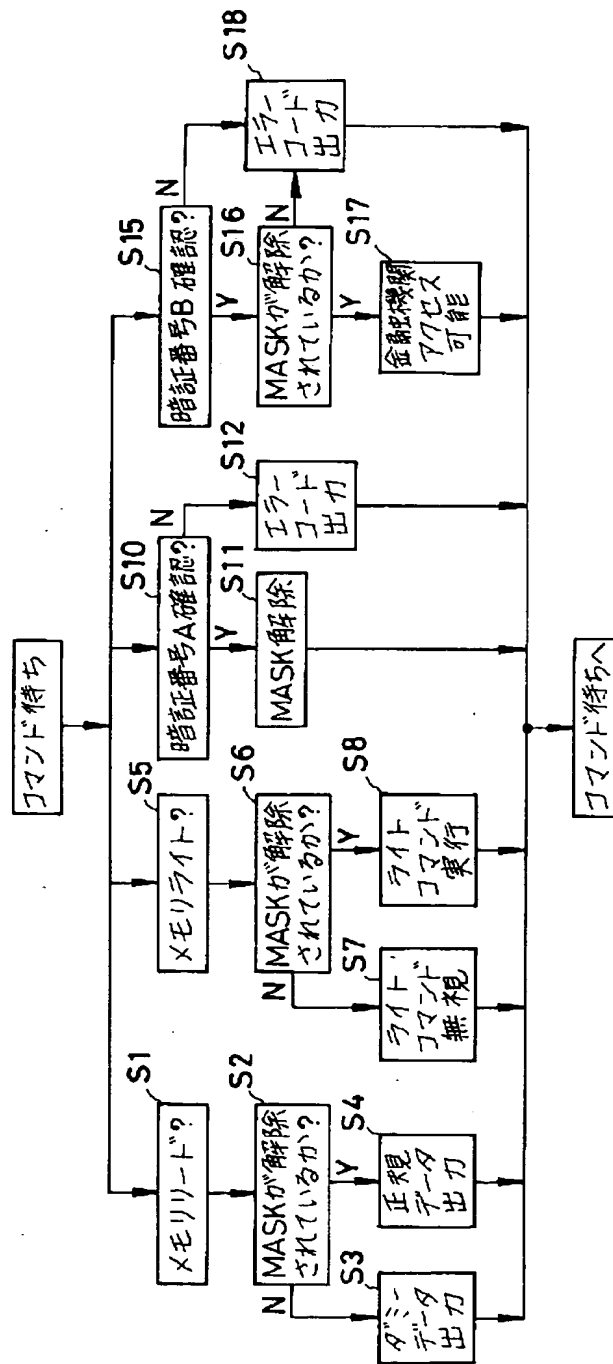
【図 5】



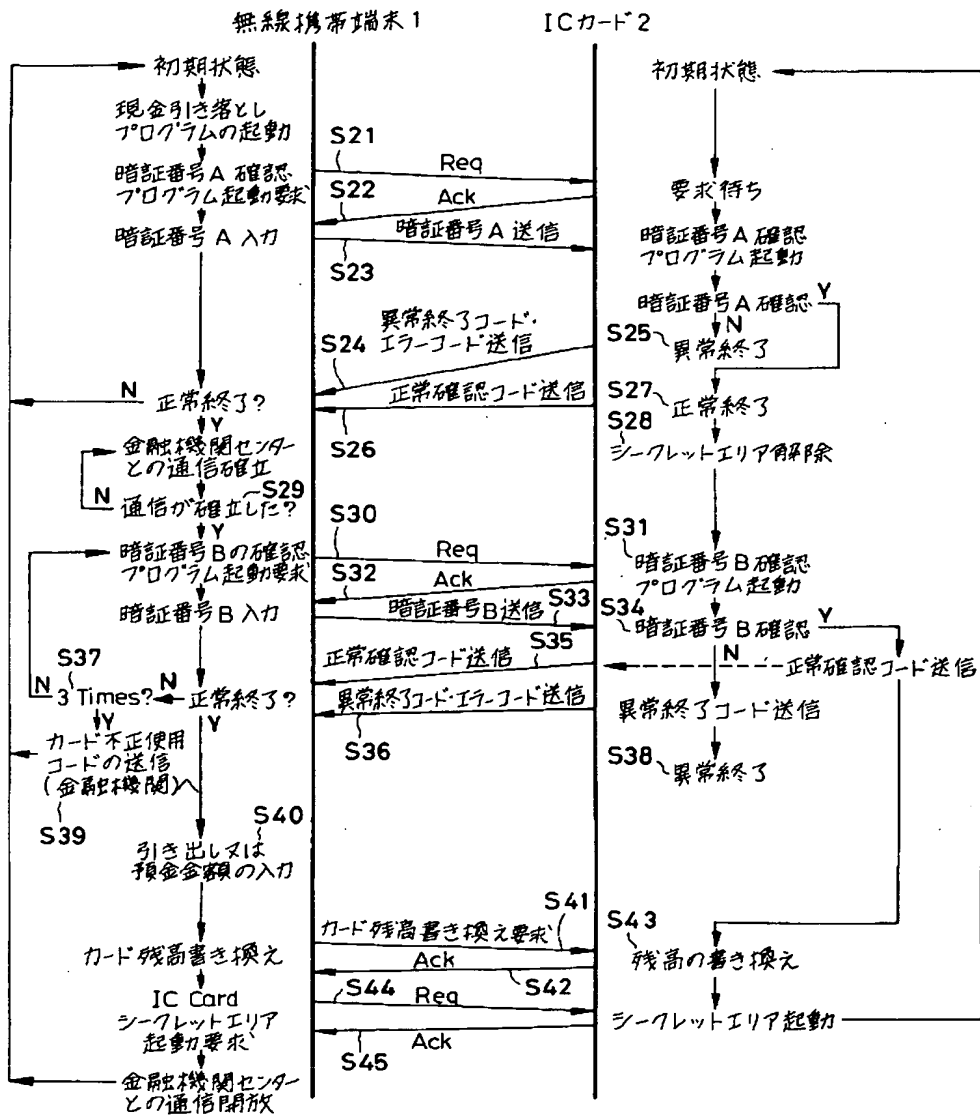
【図 6】



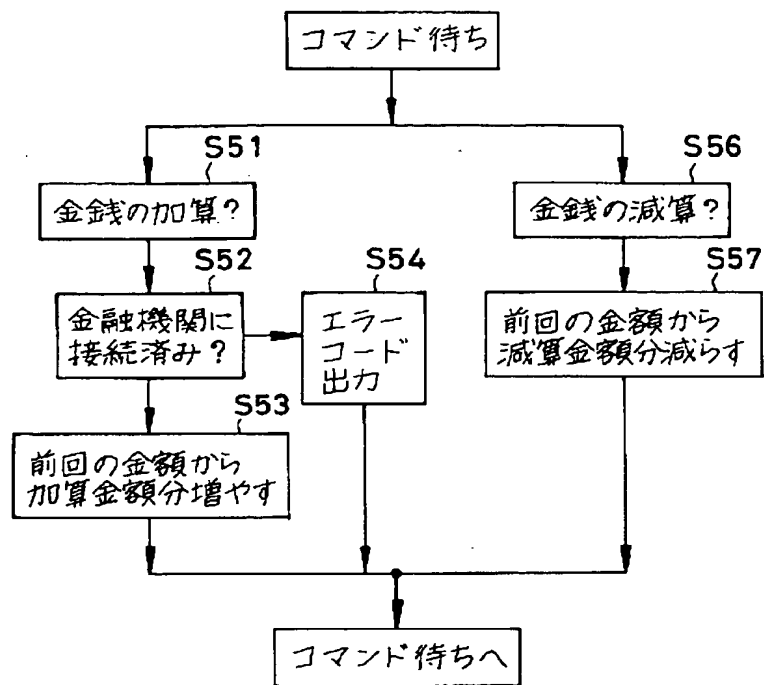
【図9】



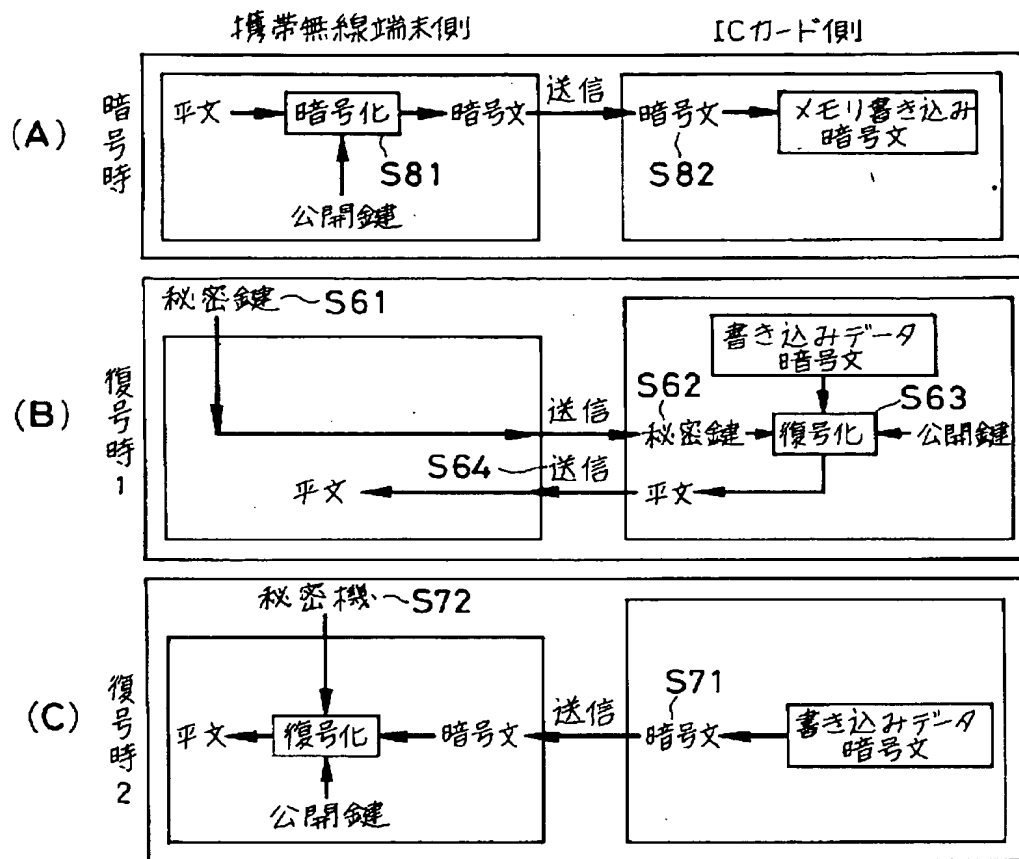
【図10】



【図 11】



【図12】



フロントページの続き

(51) Int. Cl. 6

G 0 7 D 9/00

識別記号

4 6 1

庁内整理番号

F I

G 0 7 D 9/00

G 0 6 F 15/30

技術表示箇所

4 6 1 B

3 5 0

3 6 0